CLAIMS

1. A method for analyzing a threat to system security, comprising:

identifying a threat agent having an existing access level;

using the existing access level to analyze an attack path between the threat agent and an asset; and

updating the existing access level if the analysis of the attack path between the threat agent and the asset indicates that an attack along the path would be successful.

2. A method as recited in claim 1 wherein using the existing access level to analyze an attack path between the threat agent and an asset comprises identifying a vulnerability associated with the asset.

3. A method as recited in claim 1 wherein using the existing access level to analyze an attack path between the threat agent and an asset comprises identifying an exploit method associated with a vulnerability associated with the asset.

4. A method as recited in claim 3 wherein the exploit method has associated with it a prerequisite access level required to use the exploit method to exploit the vulnerability successfully.

5. A method as recited in claim 4 wherein using the existing access level to analyze an attack path between the threat agent and an asset comprises comparing the existing access level to the prerequisite access level.

6. A method as recited in claim 4 further including determining whether a control affects the prerequisite access level.

7. A method as recited in claim 3 wherein the exploit has associated with it a resulting access level that may be attained by using the exploit to exploit the vulnerability successfully.

8. A method as recited in claim 7 further including determining whether a control affects the resulting access level.

9. A method as recited in claim 7 wherein updating the existing access level if the analysis of the attack path between the threat agent and the asset indicates that an attack along the path would be successful comprises updating the existing access level to include the resulting access level if it is determined that the threat agent has used or could use the exploit.

10. A method as recited in claim 1 further including iteratively updating the existing access level including computing a transitive closure until the analysis of the attack path

between the threat agent and the asset indicates that no further attack along the attack path would be successful.

11. A method as recited in claim 10 wherein it is determined that no further attack along the attack path would be successful if there are no further exploits associated with the asset for which the existing access of the threat agent, updated to reflect any resulting access that has been or would be attained from the successful completion of previously-analyzed exploits, is greater than or equal to the prerequisite access associated with the exploit.

12. A method as recited in claim 1 further including determining whether the asset is subject to compromise by the threat agent.

13. A method as recited in claim 1 further including determining whether a control affects the existing access level of the threat agent.

14. A method as recited in claim 13 further including updating the existing access level to reflect the affect of the control prior to using the existing access level to analyze an attack path between the threat agent and an asset.

15. A method as recited in claim 1 wherein identifying a threat agent comprises receiving from a network security system or application data comprising an identification of the threat agent.

16. A method as recited in claim 1 wherein identifying a threat agent comprises receiving from a network security system or application data that may be used to identify the threat agent.

17. A method as recited in claim 1 further including providing output data reflecting a result of the analysis of the attack path.

18. A method as recited in claim 1 wherein the output data comprises a report of the highest level of access that has been or could be achieved by the threat agent through one or more attacks along the attack path.

19. A method as recited in claim 1 wherein using the existing access level further includes evaluating recorded data to determine the attack path.

20. A method as recited in claim 1 wherein the attack path is determined by computing a transitive closure.

21. A computer program product for analyzing a threat to system security, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

identifying a threat agent having an existing access level;

using the existing access level to analyze an attack path between the threat agent and an asset; and

updating the existing access level if the analysis of the attack path between the threat agent and the asset indicates that an attack along the path would be successful.

5